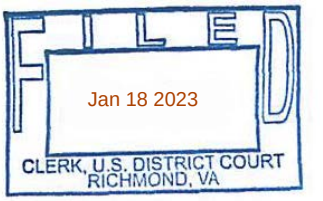
IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division



In the Matter of the Search of Information Associated with Four (4) Accounts that are Stored in Premises Controlled by Microsoft Corporation	Case No. 3:23-sw-6 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

1. I, Special Agent Travis J. Walker, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

2. I make this affidavit in support of an application for a warrant to search for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Microsoft Corporation ("Microsoft"), a company headquartered in Redmond, Washington. In accordance with Microsoft's preferred method of service, this warrant will be served on Microsoft via its Law Enforcement Portal. The information to be searched is described in the following paragraphs and in Attachment A.

3. This affidavit is made in support of an application for a search warrant under 18 United States Code ("U.S.C.") §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft to disclose to the government records and other information in its possession, pertaining to the subscriber(s) or customer(s) using its services in connection with the following Microsoft Outlook accounts:

accounting@goodvibes-llc.com;

derrick@goodvibes-llc.com;

jimmy@goodvibes-llc.com; and

ryan@goodvibes-llc.com (collectively, the "TARGET MICROSOFT ACCOUNTS").

4. I am a Special Agent with the Defense Criminal Investigative Service ("DCIS") and have been since 2022. I have over 6 years of law enforcement experience as a Special Agent with United States Government. I am assigned to the Richmond Resident Agency, and in the course of my duties, I am designated to investigate white collar crimes, and more specifically, federal fraud offenses involving the Department of Defense ("DOD").

5. As part of my official duties as an DCIS Special Agent, I am authorized to conduct investigations, carry firearms, execute warrants, make arrests, and perform other duties sanctioned by the DOD. Over the course of my career, I have conducted interviews and secured other relevant information, using a variety of investigative techniques. I am a federal law enforcement officer under the applicable provisions of the United States Code and under Rule 41(a) of the Federal Rules of Criminal Procedure. As a result, I am authorized to apply for this search warrant.

6. The facts in this affidavit come from my personal observations, my training and experience, and my conversations with agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. As set forth below, there is probable cause to believe that JAMES "JIMMY" P. MCCANN III, TROY W. BERGESON, RYAN TAYLOR, DERRICK BRENT, GOOD VIBES, LLC, and others, currently known and unknown, have committed violations of 18 U.S.C. § 1343 (Wire Fraud) (the "Target Offense"). Moreover, there is also probable cause to search the TARGET MICROSOFT ACCOUNTS described in Attachment A for the evidence and fruits of criminal activity, as described in Attachment B.

RELEVANT STATUTORY PROVISIONS

8. To establish a violation of 18 U.S.C. § 1343 (Wire Fraud), the government must prove (in relevant part) the following elements[1]:

a) The Defendant devised or intended to devise a scheme to defraud or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises that were material; and

b) For the purposes of executing the scheme, the defendant transmitted or caused to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce any writings, signs, signals, pictures, or sounds.

JURISDICTION

9. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND REGARDING MICROSOFT SERVICES

10. Based on my training and experience, I know that Microsoft provides its subscribers with Internet-based accounts that allow them to send, receive, and store emails online. Microsoft accounts are typically identified by a single username, which serves as the subscriber's

---

[1] *See* Eric Wm. Ruschky, Pattern Jury Instructions for Federal Criminal Cases, District of South Carolina § 1343 (2020 Online Edition), available at http://www.scd.uscourts.gov/pji/PatternJuryInstructions.pdf

default email address, but which can also function as a subscriber's username for other Microsoft services, such as instant messages and remote photo or file storage.

11. Based on my training and experience, I also know that Microsoft allows subscribers to obtain accounts by registering on Microsoft's website. During the registration process, Microsoft asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate email address for backup purposes, a phone number, and in some cases a means of payment. Microsoft typically does not verify subscriber names. However, Microsoft does verify the email address or phone number provided.

12. Once a subscriber has registered an account, Microsoft provides email services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. Microsoft subscribers can also use that same username or account in connection with other services provided by Microsoft.[2]

13. In general, user-generated content (such as email) that is written using, stored on, sent from, or sent to a Microsoft account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete

---

[2] Here, Microsoft's other services include: electronic communication and remote computing services such as Skype (voice calls, video calls, and SMS text messaging), Outlook Calendar (calendar and task), Office Online (cloud computing services for word processing, data processing, and presentations); OneDrive (online file storage); web browsing and search tools such as Bing Search (Internet searches), Microsoft Edge, and Internet Explorer (web browsers); Bing Maps (maps with driving directions and local business search) and other location services; online tracking and advertising tools such as Bing Ads (which facilitates targeted advertising); and Microsoft Store (which allows users to purchase and download digital content (*e.g.*, applications)). Microsoft also provides remote computing services for devices that use Windows operating systems, including security services and parental control services which collect information about the use of the devices (*e.g.*, Internet browsing history, software usage history, and other information).

an email, the email can remain on Microsoft's servers indefinitely. Even if the subscriber deletes the email, it may continue to exist on Microsoft's servers for a certain period of time.

14. Thus, a subscriber's Microsoft account can be used not only for email but also for other types of electronic communication, including instant messaging and photo and video sharing, voice calls, video chats, SMS text messaging. Depending on user settings, user-generated content derived from many of these services is normally stored on Microsoft's servers until deleted by the subscriber. Similar to emails, such user-generated content can remain on Microsoft's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on Microsoft's servers for a certain period of time. Furthermore, a Microsoft subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on Microsoft's servers.

15. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Microsoft account may be found within such computer files and other information created or stored by the Microsoft subscriber.

16. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity. Based on my training and experience, I know that providers such as Microsoft also collect and maintain information about their subscribers, including information about their use of Microsoft services. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files

that reflect usage of the account. Providers such as Microsoft also commonly have records of the IP address used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as Microsoft typically collect and maintain location data related to subscriber's use of Microsoft services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

17. Based on my training and experience, I know that providers such as Microsoft also collect information relating to the devices used to access a subscriber's account, such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by Microsoft in order to track what devices are using Microsoft's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI"). Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other Microsoft accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the Microsoft account.

18. Microsoft also allows its subscribers to access its various services through an application that can be installed on and accessed via cellular telephones and other mobile devices. This application is associated with the subscriber's Microsoft account. In my training and experience, I have learned that when the user of a mobile application installs and launches the application on a device (such as a cellular telephone), the application directs the device in question to obtain a Push Token, a unique identifier that allows the provider associated with the application to locate the device on which the application is installed. After the applicable push notification service sends a Push Token to the device, the Token is then sent to the application, which in turn sends the Push Token to the application's server/provider. Thereafter, whenever the provider needs to send notifications to the user's device, it sends both the Push Token and the payload associated with the notification (*i.e.*, the substance of what needs to be sent by the application to the device). To ensure this process works, Push Tokens associated with a subscriber's account are stored on the provider's server(s). Accordingly, the computers of Microsoft are likely to contain useful information that may help to identify the specific device(s) used by a particular subscriber to access the subscriber's Microsoft account via the mobile application.

19. Based on my training and experience, I know that providers such as Microsoft use cookies and similar technologies to track users visiting Microsoft's webpages and using its products and services. Basically, a "cookie" is a small file containing a string of characters that a website attempts to place onto a user's computer. When that computer visits again, the website will recognize the cookie and thereby identify the same user who visited before. This sort of technology can be used to track users across multiple websites and online services belonging to Microsoft. More sophisticated cookie technology can be used to identify users across devices and

web browsers. From training and experience, I know that cookies and similar technology used by providers such as Microsoft may constitute evidence of the criminal activity under investigation. By linking various accounts, devices, and online activity to the same user or users, cookies and linked information can help identify who was using a Microsoft account and determine the scope of criminal activity.

20. Based on my training and experience, I know that Microsoft maintains records that can link different Microsoft accounts to one another, by virtue of common identifiers, such as common email addresses, common telephone numbers, common device identifiers, common computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Microsoft accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Microsoft account.

21. Based on my training and experience, I know that subscribers can communicate directly with Microsoft about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Microsoft typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. In summary, based on my training and experience in this context, I believe that the computers of Microsoft are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved email for Microsoft subscribers), as well as

Microsoft-generated information about its subscribers and their use of Microsoft services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide Microsoft with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

23. As explained above, information stored in connection with a Microsoft account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a Microsoft account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

24. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Microsoft can show how and when the account was accessed or used. For example, providers such as Microsoft typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Microsoft account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the

geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the Microsoft account may indicate its user's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).[3]

PROBABLE CAUSE

A. General Scheme to Defraud

25. MCCANN, BERGESON, BRENT and TAYLOR are the co-owners and apparent principal operators of GOOD VIBES, LLC. GOOD VIBES, a Limited Liability Company based in Pleasantville, Iowa, is engaged in the business of procuring and providing products to the United States Government. GOOD VIBES has won numerous contracts and purchase orders to provide parts to the Defense Logistics Agency ("DLA") for aviation and aircraft parts, for ultimate use in DOD applications. Since 2019, GOOD VIBES has won contracts and purchase orders to provide parts to the DLA totaling approximately $5.3 million, including $2.4 million in awards in 2021. GOOD VIBES'S first bid submittal to the DLA was on or about January 21, 2019.

26. Numerous GOOD VIBES government contracts were to supply parts for government aircrafts, some of which were classified as "Critical Application Items" and "Critical

---

[3] At times, Internet services providers such as Microsoft can and do change the details and functionality of the services they offer. While the information in this section is true and accurate to the best of my knowledge and belief, I have not specifically reviewed every detail of Microsoft's services in connection with submitting this application for a search warrant. Instead, I rely upon my training and experience, and the training and experience of others, to set forth the foregoing description for the Court.

Safety Items." Per the DLA guidelines, Critical Application Items are defined as "items where failure could affect mission, performance, readiness, or safety." Similarly, Critical Safety Items are defined as "parts or support equipment for an aircraft or aviation weapon system that if they fail or malfunction could cause a catastrophic or critical failure resulting in the loss of or serious damage to the aircraft [or] an unacceptable risk of personal injury or loss of life; or an uncommanded engine shutdown that jeopardizes safety."

27. In each contract that GOOD VIBES won, it bid for a government contract to supply certain *exact* parts to DLA. Exact parts mean that the product is manufactured by, under the direction of, or under agreement with the Commercial and Government Entity Code ("CAGE") Code[4] specified in the solicitation.

28. Each of the GOOD VIBES contracts with the DLA required GOOD VIBES to have available, and to provide upon request, documentation certifying the origin of GOOD VIBES' provided parts. Such documentation – termed "traceability," and/or "certificates" – provide information on the part that is sufficient to understand the pedigree and sourcing of its component materials as well as the true manufacturer of the part. Such documentation is required to be retained by sellers of parts provided to the DLA. Per Defense Logistics Acquisition Directive ("DLAD") policy section C03, by submitting a quotation or offer, the contractor (GOOD VIBES), if it is not the manufacturer of the item, is confirming it currently has, or will obtain before delivery, and shall retain documented evidence (supply chain traceability

---

[4] A CAGE Code is a unique identifier assigned to suppliers to various government or defense agencies, as well to the government itself. In context, GOOD VIBES made representations to the DLA that parts were manufactured by particular suppliers by listing a CAGE Code associated with given parts.

documentation), as described in DLAD policy. At a minimum, the supply chain traceability documentation for the item shall include: basic item description, part number and/or national stock number, manufacturing source, manufacturing source's Commercial and Government Entity (CAGE) code, and clear identification of the name and location of all supply chain intermediaries between the manufacturer to the contractor to item(s) acceptance by the Government. The documentation should also include, if available, the manufacturer's batch identification for the item(s), such as date codes, lot codes, or serial numbers.

29. In order to bid for potential DLA contracts, GOOD VIBES utilized the DLA's Internet Bid Board System ("DIBBS"), an online application through which contractors can search for, view, and submit bids on DLA's available Requests for Quotations ("RFQs"). In order to utilize and interact with DIBBS, GOOD VIBES employees utilized their GOOD VIBES - linked email addresses, to include the TARGET MICROSOFT ACCOUNTS.

30. The TARGET MICROSOFT ACCOUNTS, according to publicly-available databases, belong to an enterprise email account registered through Microsoft. Publicly-available information confirms that this particular enterprise account – @goodvibes-llc – is hosted by Outlook.com, a Microsoft entity.

B. Whistleblower Complaints

31. In early 2022, the DLA received a whistleblower complaint alleging that GOOD VIBES was making false representations in quotes to the DLA and providing non-conforming products and/or falsified paperwork to the DLA. The whistleblower, a supplier of aircraft parts specializing in rivets for aircrafts, provided a complaint outlining a transaction involving GOOD VIBES. The allegation indicated that the whistleblower received a request for quote for a quantity of 149 "Part Number MLSP-M4-2" described as a "Rivet, Blind" from BRENT of

GOOD VIBES via e-mail. BRENT emailed the whistleblower from derrick@goodvibes-llc.com using the subject line "RE: Quote: 5320013169843". The whistleblower provided a quote for the item, but explicitly stated in the email that no certificates for the part number were available (as would be required if the parts were to be subsequently provided to the DLA). Nevertheless, BRENT accepted the quote and provided the whistleblower with a purchase order ("P.O. 22-V-9337"), dated January 19, 2022. The whistleblower suspected that GOOD VIBES intended to use these non-conforming parts to fulfil the then-open DLA contract SPE4A6-22-V-9337. Indeed, on January 18, 2022, DLA thereafter awarded GOOD VIBES the contract SPE4A6-22-V-9337 to supply a quantity of 149 "Rivet Blinds" (National Stock Number ("NSN") 5230013169843), the precise number of parts GOOD VIBES purchased from the whistleblower. The value of the contact was for $290.55. There is probable cause to believe that GOOD VIBES: (1) made knowingly false representations about the origin of parts in its bids for contracts with the DLA, including in the bid for the SPE4A6-22-V-9337 contracts; and (2) evidence of these false representations can be found in the TARGET MICROSOFT ACCOUNTS.

32. Furthermore, BRENT of GOOD VIBES contacted the whistleblower a second time regarding a quote for a quantity of 73 "Part Number GR500 AJ 06-05M" (described as a "Rivet, Blind"). BRENT emailed the whistleblower from derrick@goodvibes-llc.com using the subject line "RE: Quote: 532001246833." The whistleblower provided a quote for the item, but explicitly stated in the email that the parts were new surplus with no manufacturer certifications. Per the DLAD, new surplus requires a C04 unused former government surplus property certificate and traceability to a previous government contract. The whistleblower suspected that GOOD VIBES intended to use these non-conforming parts to fulfil the then-open DLA contract SPE4A6-22-V-062X, despite the part lacking appropriate traceability as required by the DLA. Nevertheless,

BRENT accepted the quote and provided the whistleblower with a purchase order ("P.O. 22-V-062X"), dated February 24, 2022. On February 23, 2022 TAYLOR of GOOD VIBES submitted the quote for the above mentioned contract via DIBBS using email address ryan@goodvibes-llc.com. Outlined within the DIBBS Quote Summary under "*Material Requirements*" TAYLOR certified that the parts were not "*New/ Unused Government Surplus.*"

33. Upon receipt of the whistleblower complaint, DLA began testing the parts provided by GOOD VIBES pursuant to recent government contracts and reviewing the accompanying certifications provided by GOOD VIBES. Based on this review, there is probable cause to believe that GOOD VIBES has supplied multiple non-conforming parts to the DLA and submitted falsified accompanying paperwork to conceal this fact via email. There is probable cause to believe that GOOD VIBES (as well as its employees) made misrepresentations on bid proposals via email, submitted improper traceability paperwork via email, and misrepresented information on packaging.

34. There is probable cause to believe that GOOD VIBES employees regularly relied on email correspondence – including from the TARGET MICROSOFT ACCOUNTS – to solicit parts from other companies that maintained stores of the particular parts in question. As noted more specifically below, though GOOD VIBES represented to the DLA that it would provide certified *exact* parts, GOOD VIBES ordered, received, and provided to the U.S. Government non-conforming parts of unknown pedigree.

C. Specific Instances of Suspected Fraud

Instance 1

35. In or about March 2022, GOOD VIBES provided a quote for DLA solicitation SPE4A6-22-T-996E for 731 screw sets. GOOD VIBES represented in its quote that the parts

provided had a CAGE Code 99251, corresponding with the products being manufactured by Cobham Mission Systems.

36. GOOD VIBES representative, BREANN LIGHTYLE, submitted this quote using email address accounting@ goodvibes-llc.com. GOOD VIBES represented to the Government that the parts being supplied were an exact product produced by Cobham Mission Systems. An exact product in this instance is defined in the quote submitted by GOOD VIBES under the "Notices" section, stating: "Exact product means CAGE 99251 P/N 122-10935-1: manufactured by, under the direction of, or under agreement with CAGE 99251." The notice further stated: "Any product not meeting these criteria is considered an alternate product even though it may be manufactured in accordance with the drawings and/or specifications of CAGE 99251."

37. GOOD VIBES further represented that the product they had procured was an exact match. This was accompanied with the stipulation that if traceability documentation were requested, GOOD VIBES needed to produce supporting documentation to verify the product's authenticity.

38. The DLA requested traceability documentation from GOOD VIBES on or about March 25, 2022, reflecting the quoted manufacturer, Cobham Mission Systems.

39. On or about March 25, 2022, BRENT of GOOD VIBES submitted documentation to a DLA Contract Specialist, J.S., who had requested traceability documentation for the screw sets. The documentation submitted by BRENT reflected that Cobham Mission Systems manufactured the product. BRENT submitted this documentation to the DLA using his @goodvibes-llc.com email address.

40. On March 25, 2022, J.S. contacted Cobham Mission Systems, the approved source for the screw set. J.S requested that Cobham confirm validity that GOOD VIBES procured the

screw set from Cobham. Cobham stated that they did not have a record of selling or quoting parts to GOOD VIBES. On March 29, 2022, DLA determined that the parts GOOD VIBES had quoted to the government did not possess the proper traceability that was required per the solicitation.

Instance 2

41. In or about April 2021, GOOD VIBES provided a quote for DLA solicitation number SPE5E2-21-T-2303 for the quantity of 101 "NUT, SELF-LOCKING,PL." GOOD VIBES represented that the parts provided had a CAGE code of 29372, corresponding with the part being manufactured by Howmet Global Fastening Systems, Inc.

42. BRENT submitted this quotation utilizing his @ goodvibes-llc.com email address and represented to the Government that the parts being supplied were an exact product manufactured by Howmet Global Fastening Systems, Inc., corresponding with CAGE Code 29372. The GOOD VIBES quote provided that "the material requirements were not used, reconditioned, remanufactured, or new/unused government surplus." The DLA thereafter awarded Contract SPE5E2-21-P-0747 to GOOD VIBES.

43. On April 26, 2021 a Purchase Order was issued. The order outlined a quantity of 101 "NUT,SELF-LOCKING,PL, PR 0089030465". MCCANN issued an invoice on May 8, 2021 using the jimmy@goodvibes-llc.com email address under the contract. The total amount listed in the invoice was for $1,210.99.

44. On April 18, 2022 DLA completed a product test on the product GOOD VIBES provided for contract SPE5E2-21-P-0747. The nomenclature for the test was listed as "NUT,SELF-LOCKING,PL", which was the product that was supplied from GOOD VIBES. Listed in the test report were the results, which showed that the product failed testing.

Instance 3

45. GOOD VIBES entered into Contract SPE5E4-21-P-0391 on April 12, 2021 (Solicitation SPE5EJ-21-T-4262) with DLA for the quantity of 17 "BOLT, SHEAR" (National Stock Number (NSN) 5306001265151) in April 2021. This product is listed as a Critical Application.

46. To obtain Contract SPE5E4-21-P-0391, on or about April 8, 2021, GOOD VIBES submitted a quotation to the DLA using the email address Derrick@goodvibes-llc.com. The quotation represented to the DLA that the parts being supplied were an exact product. GOOD VIBES further represented that "the material requirements were not used, reconditioned, remanufactured, or new/unused government surplus." Additionally, GOOD VIBES listed that the product they procured had an actual manufacturer CAGE Code of 56878, corresponding with the part being manufactured by SPS Technologies.

47. On or about April 12, 2021, DLA awarded Contract SPE5E4-21-P-0391 to GOOD VIBES. On April 21, 2021, DLA issued a Purchase Order under the contract. The order requested a quantity of 17 "BOLT, SHEAR PR 0088433675" pursuant to the contract.

48. On September 1, 2022, a DLA Test Coordinator and Mechanical Engineer brought Contract SPE5E4-21-P-0391 to the attention of DCIS. The Testing Coordinator related that testing revealed the bolt supplied by GOOD VIBES was not consistent with the dimensions specified in the Contract. Further, testing indicated the alloy used in manufacturing the bolt contained a composition inconsistent with the contract specifications. Additionally the testing coordinator related that markings on the bolt were inconsistent with representations made by GOOD VIBES on the bid proposal and packaging. Specifically, GOOD VIBES represented that the product was manufactured by SPS Technologies (bearing CAGE Code 56878). However, the bolt provided by GOOD VIBES contained the letters "JMP" on the face of the bolt. The testing

coordinator related that JMP is the company marking of J.M Precision, Inc, bearing CAGE Code 0JV78. The testing coordinator further stated the packaging provided by GOOD VIBES identified CAGE Code 56878, SPS Technologies, was the true parts manufacturer (as was required by contract); however, the parts provided were inconsistent with GOOD VIBES' representation.

D. Summary of Probable Cause

49. There is probable cause to believe that GOOD VIBES has made knowingly false and material misrepresentations in its contract solicitations to the DLA about the source, origin, and traceability of various parts provided to the DLA– specifically, by representing that GOOD VIBES would provide "exact parts" and subsequently delivering patently non-conforming parts (in some cases, on items of critical safety to airplanes and/or personnel). This probable cause is based on the assertions of the whistleblower, who provided parts to GOOD VIBES without certificates and flagged for GOOD VIBES that such parts lacked traceability; yet, the whistleblower reports that GOOD VIBES likely used these non-conforming parts in a contemporaneous DLA bid solicitation for the exact same number of those very same part types, which GOOD VIBES won within days of the whistleblower coordinating the sale of parts to GOOD VIBES. The probable cause is also based on GOOD VIBES' history of soliciting DLA contracts, subsequently delivering non-conforming parts (in some cases, on items that are critical to safety of airplanes and/or personnel), and certifying that non-conforming parts satisfied origin requirements.

50. At the time of this report, more than half of the products selected for testing by DLA have failed testing. To be sure, other parts provided by GOOD VIBES have passed DLA testing.

51. There is probable cause to believe that GOOD VIBES employees regularly utilized their GOOD VIBES-provided email, to include the TARGET MICROSOFT ACCOUNTS, in the execution of the scheme to defraud. GOOD VIBES employees used TARGET MICROSOFT ACCOUNTS to correspond with suppliers to obtain parts that were eventually sold to the DLA, to solicit and bid for contracts with the DLA, and to communicate with the DLA, including on logistical matters and regarding GOOD VIBES providing parts to DLA.

52. Your affiant has previously provided Microsoft with a preservation request for the TARGET MICROSOFT ACCOUNTS on May 3, 2022. In general, an e-mail that is sent to a Microsoft account subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Microsoft's servers for a certain period of time.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

53. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. The warrant authorizes such a review anywhere within the United States.

54. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by

serving the warrant on Microsoft. Because the warrant will be served on Microsoft, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR NON-DISCLOSURE AND SEALING

55. The government requests, pursuant to the preclusion of notice provisions of Title 18, United States Code, Section 2705(b), that Microsoft be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of the search warrant for such period as the Court deems appropriate. The government submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation.

56. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of the Application for a Search Warrant. Premature disclosure of the contents of this affidavit and related documents may have a negative impact on the continuing investigation and may jeopardize its effectiveness.

CONCLUSION

57. There is probable cause to believe evidence of wire fraud (18 U.S.C. § 1343) (Wire Fraud) and communications about this offense will be found in the TARGET MICROSOFT ACCOUNTS. Based on the forgoing, I request that the Court issue the proposed search warrant.

Respectfully submitted,

WALKER.TRAVIS.JAMES.1610999260

Digitally signed by WALKER.TRAVIS.JAMES.1610999260
Date: 2023.01.17 12:17:34 -05'00'

Travis J. Walker
Special Agent
Defense Criminal Investigative Service

Subscribed and sworn to me by telephone
on this date JAN. 18, 2023

HON. MARK R. COLOMBELL
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

In the Matter of the Search of Information Associated with Four (4) Accounts that are Stored in Premises Controlled by Microsoft Corporation	Case No. 3:23-sw-6 **Filed Under Seal**

ATTACHMENT A
Property to be Searched

This warrant applies to information associated with the follow accounts:

Microsoft Email Address
accounting@goodvibes-llc.com
derrick@goodvibes-llc.com
jimmy@goodvibes-llc.com
ryan@goodvibes-llc.com

(collectively, the "TARGET MICROSOFT ACCOUNTS").

Said information is stored at premises owned by Microsoft Corporation ("Microsoft"), a company headquartered in Redmond, Washington.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

In the Matter of the Search of Information Associated with Four (4) Accounts that are Stored in Premises Controlled by Microsoft Corporation	Case No. 3:23-sw-_____ **Filed Under Seal**

ATTACHMENT B
Particular Things to be Seized

1. The items to be seized are evidence and fruits of violations of the following federal statute (the "Target Offense"): 18 U.S.C. § 1343 (Wire Fraud).

I. Information to be Disclosed by Microsoft

2. To the extent that the information described in Attachment A is within the possession, custody, or control of Microsoft, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to Microsoft, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Microsoft is required to disclose the following information to the government for the accounts listed in Attachment A:

a. all records or other information pertaining to the account, including, but not limited to, all files and content, stored by Microsoft in relation to the TARGET MICROSOFT ACCOUNTS;

b. all information in the possession of Microsoft that might identify the subscribers related to the TARGET MICROSOFT ACCOUNTS, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. all records pertaining to the types of services and applications associated with the TARGET MICROSOFT ACCOUNTS;

d. all records associated with any Microsoft OneDrive account connected to the TARGET MICROSOFT ACCOUNTS, including all files stored in OneDrive and records related to those accounts with which the TARGET MICROSOFT ACCOUNTS shared those files, including the associated email address, file name, date(s) when the file(s) was/were shared, and any log data showing creation/modification dates associated with the file(s);

e. all Skype aliases and phone numbers associated with the TARGET MICROSOFT ACCOUNTS;

f. all Skype contact lists and any available archived Skype chat history associated with the TARGET MICROSOFT ACCOUNTS;

g. all records pertaining to communications between Microsoft and any person regarding the TARGET MICROSOFT ACCOUNTS, including contacts with support services and records of actions taken; and

h. records of session times and durations, as well as any temporarily assigned network address associated with the TARGET MICROSOFT ACCOUNTS, including all IP addresses assigned to the subscriber(s) for a particular session and the remote IP address from which the subscriber(s) connected.

2. Microsoft is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be Seized by the Government

3. All information described above in Section I that constitutes evidence and fruits of violations of the Target Offense, **from January 1, 2019 to the present**, including information pertaining to the following matters:

a. Evidence that helps determine: 1) how and when the email account was accessed and/or used; 2) the geographic and chronological context of the account access and/or use; 3) events and/or transactions relating to the Target Offense; and evidence demonstrating any connection and/or relationship to, or culpability for, the Target Offense by the email account's owner(s) or user(s);

b. Evidence indicating the email account owner's state of mind as it relates to the Target Offense;

c. The identity of the person(s) who created or used the TARGET MICROSOFT ACCOUNTS, including records that help reveal the whereabouts of such person(s); and

d. The identity of the person(s) who communicated with the TARGET MICROSOFT ACCOUNTS about matters relating to the Target Offense, including records that help reveal the whereabouts of such person(s).

4. This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence and fruits of the Target Offense described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts located anywhere in the United States. Pursuant to this warrant, the Defense Criminal Investigative Service may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

III. Filter Team Protocols

5. If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do not involve an

attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (e.g., the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team. This investigation is presently covert and the government believes that the subject of the search is not aware of this warrant.